APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/525,510	03/15/2000	Marcus Peinado	MSFT-0135/147325.1	9494

7590   09/03/2002

Steven H Meyer
Woodcock Washburn Kurtz Mackiewicz & Norris LLP
One Liberty Place 46th Floor
Philadelphia, PA   19103

EXAMINER
BACKER, FIRMIN

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 09/03/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

-- The MAILING DATE of this communication appears on the c ver sh et with the correspondence address --

Peri d for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *15 March 2000* .

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disp sition of Claims

4) ☒ Claim(s) *1-46* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-46* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

　　If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a) ☐ All b) ☐ Some * c) ☐ None of:

　　　　1. ☐ Certified copies of the priority documents have been received.

　　　　2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

　　　　3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

　　a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

This is in response to a letter for patent filed on March 15th, 2000 in which claims 1-46 are

presented for examination. Claims 1-46 are pending in the letter.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United
States before the invention thereof by the applicant for patent, or on an international application by another who
has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention
thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999

(AIPA) do not apply to the examination of this application as the application being examined

was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C.

122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment

by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2.   Claims 1-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Matsuzaki et al

(U.S. Patent No. 6,058,476).

3.   As per claims 1 and 24, Matsuzaki et al teach a method/computer readable medium for

releasing (*transmission system/method*) digital content (*digital copyrighted material*) to a

rendering application (*a first device, 51, 110*), the rendering application for forwarding the digital

content to an ultimate destination (*second device, 52, 111*) by way of a path (*communication*

cable 116) there between, the path being defined by at least one module (*SCSI controller, 121,*

130), the digital content (*digital copyrighted material*) initially being in an encrypted form (*see*

fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9) comprising performing an

authentication (*authentication*) of at least a portion of the path (*the device*) to determine whether

each defining module thereof is to be trusted to appropriately handle the digital content passing

there through (*see column 6 lines 22-50*) decrypting (*decryption unit*) the encrypted digital

content if in fact each such defining module is to be trusted (*column 6 line 51-64*), and

forwarding (*transmitting*) the decrypted digital content to the rendering application for further

forwarding to the ultimate destination by way of the authenticated path (*see column 5 lines 45-*

67, 9 line 29-10 line 4, 18 line 21-67).

4.   As per claims 2 and 25, Matsuzaki et al teach a method/computer readable medium

further comprising scrambling the digital content upon such digital content being outputted from

the rendering application to the path such that the scrambled digital content enters the user mode

portion of the path, such scrambled digital content then passing through the modules that define

the user mode portion of the path and transiting from the user mode portion to the kernel portion

of the path; and de-scrambling the scrambled digital content upon such scrambled digital content

transiting from the user mode portion to the kernel portion (*see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9*).

5.   As per claims 3 and 26, Matsuzaki et al teach a method/computer readable medium comprising de-scrambling the scrambled digital content by way of a de-scrambling module (*see column 6 lines 22-50*).

6.   As per claims 4 and 27, Matsuzaki et al teach a method/computer readable medium comprising de-scrambling the scrambled digital content in the kernel portion of the path *(see column 5 lines 45-67, 9 line 29-10 line 4, 18 line 21-67)*.

7.   As per claims 5 and 28, Matsuzaki et al teach a method/computer readable medium comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing there through *(see column 5 lines 45-67, 9 line 29-10 line 4, 18 line 21-67)*.

8.   As per claims 6 and 29, Matsuzaki et al teach a method/computer readable medium wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing there through (*see column 6 lines 22-50*).

9.   As per claims 7 and 30, Matsuzaki et al teach a method/computer readable medium

further comprising scrambling the digital content upon such digital content being outputted from

the rendering application to the path such that the scrambled digital content enters the user mode

portion of the path, such scrambled digital content then passing through the modules that define

the user mode portion of the path and transiting from the user mode portion to the kernel portion

of the path; and de-scrambling the scrambled digital content upon such scrambled digital content

transiting from the user mode portion to the kernel portion (*see fig 3, 9, 10, 11, column 11 line

11-61, 22 line 42-23 line 9*).

10.   As per claims 8 and 31, Matsuzaki et al teach a method/computer readable medium

comprising de-scrambling the scrambled digital content by way of a de-scrambling module *(see

column 5 lines 45-67, 9 line 29-10 line 4, 18 line 21-67)*.

11.   As per claims 9 and 32, Matsuzaki et al teach a method/computer readable medium

comprising de-scrambling the scrambled digital content in the kernel portion of the path (*column

6 line 51-64)*.

12.   As per claims 10 and 33, Matsuzaki et al teach a method/computer readable medium

wherein performing the authentication comprises traversing the at least a portion of the path to

develop a map of each module in the path; and authenticating each module in the map (*column 6

line 51-64)*.

13.   As per claims 11 and 34, Matsuzaki et al teach a method/computer readable medium

wherein performing the authentication further comprises ignoring each module not in the map

(*see column 6 lines 22-50*).

14.   As per claims 12 and 35, Matsuzaki et al teach a method/computer readable medium

wherein performing the authentication comprises authenticating an initial module determining all

first destination modules that receive data from such initial module authenticating each such first

destination module, determining all second destination modules that receive data from each such

first destination module, iteratively repeating the authenticating and determining steps for third,

fourth, fifth, etc. destination modules until each module in such at least a portion of the path

has been determined and authenticated (*see fig 3, 9, 10, 11, column 11 line 11-61, 22 line

42-23 line 9*).

15.   As per claims 13 and 36, Matsuzaki et al teach a method/computer readable medium

wherein authenticating the initial module comprises authenticating a module in the at least a

portion of the path that is to receive the digital content before any other module in the at least a

portion of the path, whereby the initial module leads to fully determining all other modules that

define the at least a portion of the path (*see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23

line 9*).

16.   As per claims 14 and 37, Matsuzaki et al teach a method/computer readable medium comprising employing a database device to keep track of all modules determined to be in the at least a portion of the path, whereby already-determined modules in the at least a portion of the path can be recognized (*see column 6 lines 22-50*).

17.   As per claims 15 and 38, Matsuzaki et al teach a method/computer readable medium wherein performing an authentication comprises for each module in the at least a portion of the path: receiving from the module a certificate as issued by a certifying authority; and determining from the received certificate whether such received certificate is acceptable for purposes of authenticating the module (*column 6 line 51-64*).

18.   As per claims 16 and 39, Matsuzaki et al teach a method/computer readable medium wherein performing an authentication further comprises checking a revocation list to ensure that the received certificate has not been revoked (*see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9*).

19.   As per claims 17 and 40, Matsuzaki et al teach a method/computer readable medium further comprising receiving the revocation list from a certifying authority; storing the received revocation list in a secure location (*see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9*).

20.   As per claims 18 and 41, Matsuzaki et al teach a method/computer readable medium

wherein performing an authentication further comprises refusing to decrypt the encrypted digital

content if at least one module in the at least a portion of the path fails to provide an acceptable

certificate (*see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9*).

21.   As per claims 19 and 42, Matsuzaki et al teach a method/computer readable medium

wherein performing an authentication further comprises decrypting the encrypted digital content

if all the modules in the at least a portion of the path provide an acceptable certificate *(see*

column 5 lines 45-67, 9 line 29-10 line 4, 18 line 21-67).

22.   As per claims 20 and 43, Matsuzaki et al teach a method/computer readable medium

wherein performing an authentication further comprises, for each module in the at least a portion

of the path that fails to provide an acceptable certificate defining a sub-portion of the path

including the non-providing module, scrambling the digital content upon such digital content

entering the tunnel portion of the path. such scrambled digital content then passing through the

modules that define the sub-portion of the path; and de-scrambling the scrambled digital content

upon such scrambled digital content exiting from the sub-portion of the path; and declaring the

sub-portion trustworthy (*see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9*).

23.   As per claims 21 and 44, Matsuzaki et al teach a method/computer readable medium

wherein the path includes a user mode portion and a kernel portion, the method comprising

performing an authentication of the user mode portion of the path and of the kernel portion of the

path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing there through *(see column 5 lines 45-67, 9 line 29-10 line 4, 18 line 21-67)*.

24.   As per claims 22 and 45, Matsuzaki et al teach a method/computer readable medium wherein the path includes a tunneled portion, the method further comprising scrambling the digital content upon such digital content entering the tunneled portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the path; and de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the path, and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing there through, an authentication of the tunneled portion being unnecessary *(see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9)*.

25.   As per claims 23 and 46, Matsuzaki et al teach a method/computer readable medium wherein the path includes a user mode portion, a kernel portion, and a tunneled portion in the user mode portion, the method further comprising scrambling the digital content upon such digital content entering the tunneled portion of the user mode portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the user mode portion of the path, and de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the user mode portion of the path and

wherein performing an authentication comprises performing an authentication of at least a

portion of the path external to the tunneled portion of the user mode portion of the path to

determine whether each defining module thereof is to be trusted to appropriately handle the

digital content passing there through, an authentication of the tunneled portion being unnecessary

(see fig 3, 9, 10, 11, column 11 line 11-61, 22 line 42-23 line 9).

Conclusion

26.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

      a.   *Sullivan et al (U.S. Patent No. 6,069,647) teach a system comprises an interface*

unit coupled to a programmable unit. The interface unit is capable of containing a time-

sensitive key. The programmable unit receives digital content from the interface unit

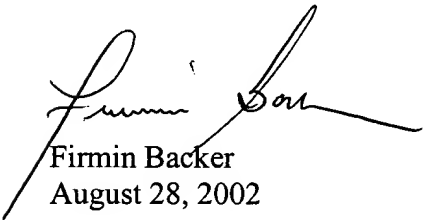*upon establishing that the time-sensitive key is also contained therein.*

      b.   *Berson et al (U.S. Patent 5,949,879) teach an inventive providing a secure system*

for authenticating information. The information may be in the form of a printed document

or stored in a electronic format (disk, smart card, etc.). This invention provides for a

audit-able, secure environment for the generation of cryptographically protected digital

data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammel can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

Firmin Backer
August 28, 2002

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600